UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,828	06/07/2000	Eric J. Sprunk	D02302	9516

7590 11/15/2007

General Instrument Corporation
101 Tournament Drive
Horsham, PA 19044

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
11/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/588,828	SPRUNK ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/31/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2-8* is/are allowed.

6)☒ Claim(s) *9-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is written in responding to the Request for Continued Examination (RCE) dated on 08/31/2007.

2. Claims 2- 11 have been submitted for examination.

3. Claims 2-11 are pending.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith U.S. Patent 5,548,648) and further in view of Matyas et al. (U.S. Patent 5,265, 164).

6. As per claim 9, York-Smith discloses a method for decrypting information in a message that can be authenticated, the message containing a first cipher block and a second cipher block **[EDS1 and EDS 2 from the data block D in Fig. 3]** subdivided from an block combined with information in the message **[Fig. 3, where CBs are separated from EDs]**, the second cipher block being combined with a residual field and

a second block **[(Col 3 lines 45-55, and Figure 3), *where CB2 is combined with ED2 and random number X*]**, the method comprising:

decrypting at least the cipher residual block of the message to obtain a representation of a second authentication block **[(lines 65-67, Col.2 and lines 3-9, Col. 3 and Fig. 6)]**;

decrypting the first cipher block and the second cipher block to obtain at least a representation of a first authentication block **[(lines 65-67, Col.2 and lines 3-9, Col. 3 and Fig. 6)]**; and

York-Smith does not expressly disclose the blocks are used as authentication block and the second cipher block being encrypted for a cipher residual block, and comparing the authentication block value to the expected value to authenticate the message. However Matyas et al. disclose the second part of the block contains authenticator block, the authenticator block is encrypted **[(Fig. 20)]**, and comparing the authenticator block value to the expected value (by utilizing the on-way hash algorithm) to authenticate the message **[(lines 38-50, Col. 11; lines 24-29 and 51-67, Col. 21; lines 44-54, Col. 38; lines 33-39, Col. 40; Fig. 20)]**.

York-Smith and Matyas et al. are analogous art because they are from similar technology relating to communication and security. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine York-Smith and Matyas since one would have been motivated to have cryptographic systems and methods for use in data processing systems to enhance security (lines 10-11, Col. 1 from Matyas et al.). Therefore, it would have been obvious to combine York-Smith with Matyas et al. to obtain the invention as specified in claim 9.

10. As per claim 10, York-Smith and Matyas et al. disclose the method of the claim 9, wherein the second authentication block comprises one or more bits **[(Fig. 3 from York-Smith) and (lines 24-29, Col. 21 from Matyas et al.)]**.

11. As per claim 11, York-Smith and Matyas et al. disclose the method of claim 9, wherein the second authentication block comprises one or more bits forming a null value **[(Fig. 3 from York-Smith) and (lines 24-29, Col. 21 from Matyas et al.), *where bits are either 1 or 0 (null-vale)*]**.

Allowable Subject Matter

6. Claims 2-8 are allowed.

7. Independent Claims 2, 5, and 6:

   a. The primary reasons for the allowance of the independent 2 and 5-6 are inclusion of the following limitations that are not found in the prior art and they are not uniquely distinct features. The cited closest prior art by Yorke-Smith (U.S. Patent 5,548,648) and Koopman (U.S. Patent 5,619,575) are presented in the prior Office Action. These prior art, singularly or in combination, fail to anticipate or render the recited limitation on encrypting the second subblock and residual portion together with the second authentication block using a second key to form a cipher residual block and providing at least the first cipher subblock of the designated cipher block of the message for authentication in Claims 2 and 5-6.

8. Dependent Claims 3-4 and 7-8:

a. Claims 3-4 and 7-8 are claims that depend on Claims 2 and 6, respectively. Therefore, they are allowable on the basis that Claims 3-4 and 7-8 also contain all the unique features that are not found in the closest abovementioned prior art.

Conclusion

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

b. Rogaway (U.S. Patent 5,491,749) discloses message authentication codes (MACs) are utilized in cryptography to assure the authenticity of communications. These types of operations are frequently referred to as "message authentication operations". Typically, message authentication operations permit a receiver to validate a message's origin and destination, contents, timeliness, and sequence relative to other messages flowing between communicants. While a variety of algorithms may serve to perform the method authentication code (MAC) operations, the best known and official scheme is 8 documented in the DES MODES OF OPERATION publication, more specifically identified as the Federal Information Processing Standards Publication, FIPS PUB 81, published by the National Bureau of Standards on Dec. 2, 1980. Preferably, the Cipher Block Chaining (CBC) mode is used to encrypt plaintext, which must be padded (for example, with zero bits) if necessary to make it a

multiple of sixty-four bits in length. The MAC consists of the last k bits of cyphertext, the rest of which is discarded. This process is discussed in an article by C. H. Meyer and S. M. Matyas, entitled "Cryptography: A New Dimension in Computer Data Security", published by John Wiley & Sons, of New York, in 1982. The utilization of the DES algorithm in the Cipher Block Chaining mode of operation demonstrates a well-established forward error propagating property; therefore, the change of even so much as a single bit in the plaintext would cause an unpredictable change in every bit in the MAC with the probability of fifty percent for each bit. Utilizing a MAC which is k-bits long, and the MAC is transmitted along with the associated message to be authenticated, and that portion is recomputed on the received message at the destination.

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER